# Identity Fraud, Inc. SB Article 1

**SMALL BUSINESSES ABLE TO OPTIMIZE IDENTITY CRIME DEFENSES**

According to history scholars, the first imposter was Smerdis, dating back nearly 2,500 years. We anticipate that imposters, identity and data thieves will continue in our time as well. Because identity crimes cannot be stopped entirely, organizations need to optimize their resources in the fight against identity crimes by investing in solutions until the benefits no longer justify the costs.

While optimization is a worthy pursuit in theory, it is easier said than done. Small and medium sized businesses need to begin by using resources where they have the greatest return on their investment and then focus remaining resources on achieving smaller, yet valued benefits.

---

Figure I illustrates, in part and without showing marginal benefit and marginal cost curves, how investments in prevention and security relate to benefits.

- From Point A to Point B, the marginal benefit of increased investments are worthwhile, and outweigh their marginal cost.

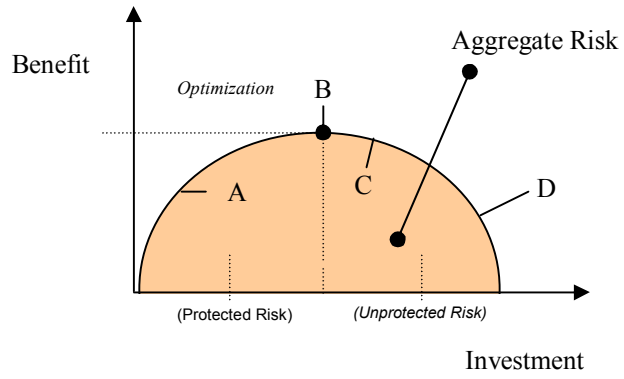
- At Point C, additional investments do not result in worthwhile benefits as costs begin to exceed the additional benefits gained.

- At Point D, more investment actually reduces the aggregate benefits, i.e. too much security may actually harm productivity and operations.

- Optimization occurs at Point B, where marginal benefit equals marginal cost.

Figure I - *IFI Risk Optimization Curve™*

(Graph is for illustration purposes only)




The Risk Optimization Curve or "ROC" supports the understanding and theory that risks are never fully eliminated because investment to reduce risk and increase benefits will cease at Point B, the point of optimization. Indeed, the ROC further indicates that achieving a point of optimization leaves a significant amount of *unprotected risk* to remain. In theory, this risk shall always remain as long as operations continue. Because risk will always exist, contracts, insurance and other risk transfer tools are created to efficiently accommodate for risk transfer.

We present our ROC to help illustrate that managing data theft risks, like any risk, should entail the efficient use of prevention resources up to their optimal point and that insurance and/or other risk transfer tools are necessary to allow remaining risks to be transferred. Ultimately, managing risks in this comprehensive fashion removes uncertainties and the catastrophic loss events that can destroy the business. Proper management of risks allows the business to prosper.

---

With identity crimes having a meaningful impact on daily operations, they also have the potential to cause catastrophic loss. The risks are no longer about single transactions that one might ignore or dismiss as a cost of doing business, rather, the risks today relate to the collection, use, and disclosure of information, which is a part of every business. As consumers, our information is everywhere and the pressures to secure that information has reached a critical point.

**Investment in Education**

Identity Fraud, Inc. helps small business organizations optimize their resources by first focusing on a major investment and asset that every organization maintains, employees. Employees represent an organization's front line of defense against fraud. IFI education programs allow organizations to effectively train employees with a negligible level of expense, allowing for a maximum return on investment. Having a single employee stop one or a few potential fraud attempts will easily justify an investment in IFI small business solutions.

Fraud prevention training produces other benefits for organizations as well. Employees that see an investment in training better understand the importance the organization places on fraud prevention and information privacy and security. In turn, employers can expect more from their employees as a result of training and hold employees accountable for their actions. A significant by product of fraud prevention training is deterrence. Employees that may want to take advantage and steal from the organization will need to overcome the internal controls and attention being focused on crime prevention. With over 70% of thefts occurring from within organizations, deterrence plays a significant role in reducing losses.

**Gap Analysis / Organizational Assessments**

Identifying potential gaps and exposures in polices, procedures, or operations can significantly benefit an organization. Gaps may be as simple as not using a computer firewall or not properly shredding sensitive information. However, understanding and evaluating organizational exposures requires knowledge and education to be effective. Tools that are able to enhance a review help save time and money.

IFI provides three levels of information security risk assessment protocols that are designed to maximize an organization's return on investment. Years of experience and effort have gone into developing the protocols and yet they are included in IFI small business solutions and allocated a negligible cost. By utilizing the protocols and other education for managers or owners, cost savings are realized while important and specific exposures are uncovered that result in legitimate gap analysis and exposure identification. By being inexpensive and simple to use, organizations achieve a high rate of return on investment.

**Remaining Risk**

As indicated in Figure I and in practice, some degree of risk will always remain in conducting business. For risks that do remain and are not otherwise preventable by an efficient use of technology and related resources, it is likely both economical and justified to transfer risk to insurance products. That's why IFI's small business solutions include business identity fraud insurance and information security and privacy liability insurance. When loss does occur, insurance can protect the organization's bottom line.

In summary, organizations should deploy resources to a point where the value no longer justifies the cost. IFI solutions are designed to maximize organizational results at a cost that remains beneficial. By addressing remaining risk with insurance products, organizations can effectively optimize their defenses against fraud.

###